

最近の情勢を踏まえた
我が国のサイバーセキュリティ政策について

内閣サイバーセキュリティセンター
副センター長 吉川徹志

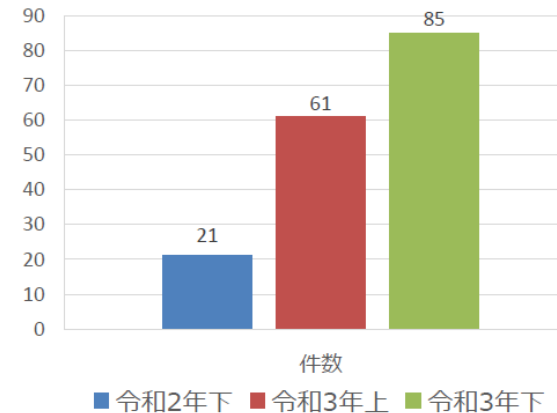
2022年6月17日

ランサムウェアやEmotetによる被害拡大

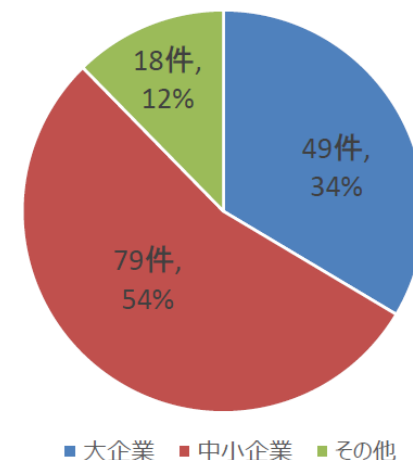
ランサムウェア

- ランサムウェアは「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語。感染したパソコンのデータを暗号化するなど使用不可にし、その**解除と引換えに金銭を要求**する。
- 近年は新たなランサムウェアとして、システムの復旧に対する**金銭要求**に加え、窃取した**データを公開しない見返りの金銭要求**も行う**二重の脅迫が発生**している。
- 国内事例として、企業・団体等におけるランサムウェア被害として、令和3年に全国の都道府県警察から警察庁に報告があった件数は**146件**であり、前年と比較可能な7～12月だけで**4倍と大幅に増加**。
- 被害件数(146件)の内訳は、**大企業が49件（34%）**に対して、**中小企業は79（54%）と過半数超**。

企業・団体等におけるランサムウェア被害の報告件数の推移



ランサムウェア被害の被害企業・団体等の規模別報告件数（令和3年）

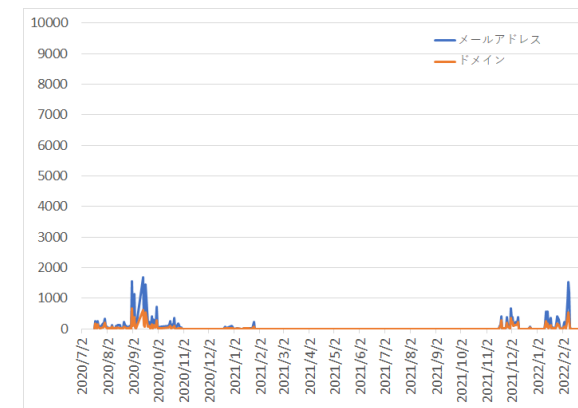


（データ出所）経済産業省「2022年4月11日産業サイバーセキュリティ研究会」資料、警察庁「令和3年におけるサイバー空間をめぐる脅威の情勢等について（2022年2月10日）」を基にNISC作成

Emotet

- 2021年11月から再開したEmotetの攻撃活動が、**2022年2月より急増**しており、国内企業・組織から感染被害が公表されている。
- 2022年3月のEmotetに感染しメール送信に悪用される可能性のある.jpメールアドレス数が2020年の感染ピーク時の**約5倍以上に急増**。
- Emotetの攻撃メールの手口としては、**Excelファイルのマクロ機能の悪用、パスワードZIPファイルの悪用、URLリンクのクリックの誘導等**がある。

Emotetに感染しメール送信に悪用される可能性のある.jpメールアドレス数

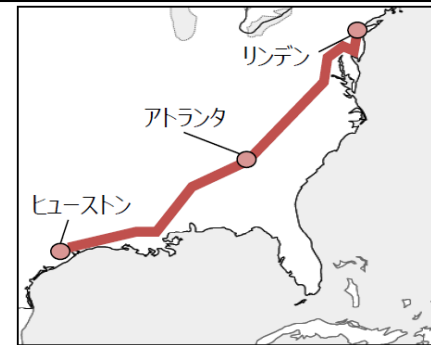


（データ出所）JPCERT/CC「マルウェアEmotetの感染拡大に関する注意喚起(2022年3月14日)」を基にNISC作成

米国におけるランサムウェア被害及び注意喚起等の対応状況

石油パイプライン大手

- 米国の専門機関によれば、米国における重要インフラ事業者等への攻撃のうち、約1割は制御系システムにまで影響を及ぼした。
- 一例として、2021年5月には、米石油パイプライン大手がランサムウェア攻撃を受け、全てのパイプラインを一時停止。米運輸省が燃料輸送に関する緊急措置の導入を宣言する事態に陥った。



(データ出所) 経済産業省「2022年4月11日産業サイバーセキュリティ研究会」資料を基にNISC作成

米国大統領による声明

- 2022年3月21日（米国東部時間）、**米国バイデン大統領が国内の重要インフラ事業者等に対して、ロシアのサイバー攻撃への警戒を呼びかける声明**を発出。

バイデン大統領による「国家のサイバーセキュリティに関する声明」（2022年3月21日ホワイトハウス）（抜粋）

（略）我々の作業を加速するための重要な瞬間である。私は、ロシアが米国に対して悪意のあるサイバー活動を行う可能性について警告してきた。（中略）本日、私の政権は、**ロシア政府が潜在的なサイバー攻撃の選択肢を検討している、という進化している情報(evolving intelligence)に基づいて、これらの警告を繰り返し表明する。**

（中略）**重要なインフラの所有者と運営者は、デジタルドアをロックする取り組みを加速させる必要があります。**（略）まだそうしていないのであれば、私は、民間部門のパートナーに対して、昨年我々が共に開発したベストプラクティスを実施することによって、サイバー防御を直ちに強化することを強く求めます。（略）**私たちの時代を決定づける脅威の1つに対処するために、誰もが役割を果たす必要があります。**今日の警戒と緊急性は、明日の攻撃を防止または軽減することができます。

（国立研究開発法人情報通信研究機構(NICT)による翻訳を基に作成）

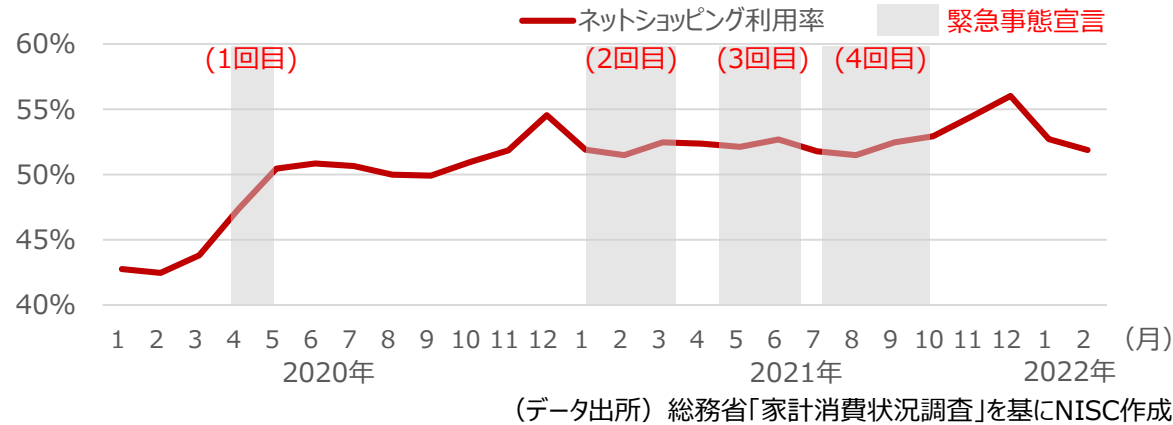
- あわせてファクトシートを公表し、企業等に対してサイバー防衛を強化する具体策※を提示。

※ 多要素認証の使用、セキュリティパッチの適用による脆弱性対策、データのバックアップ、緊急時に備えた計画の策定と演習の実施、データの暗号化、従業員に対する教育、CISA等が提供する技術情報等の活用 等

環境変化、国際情勢から見たリスク（１）

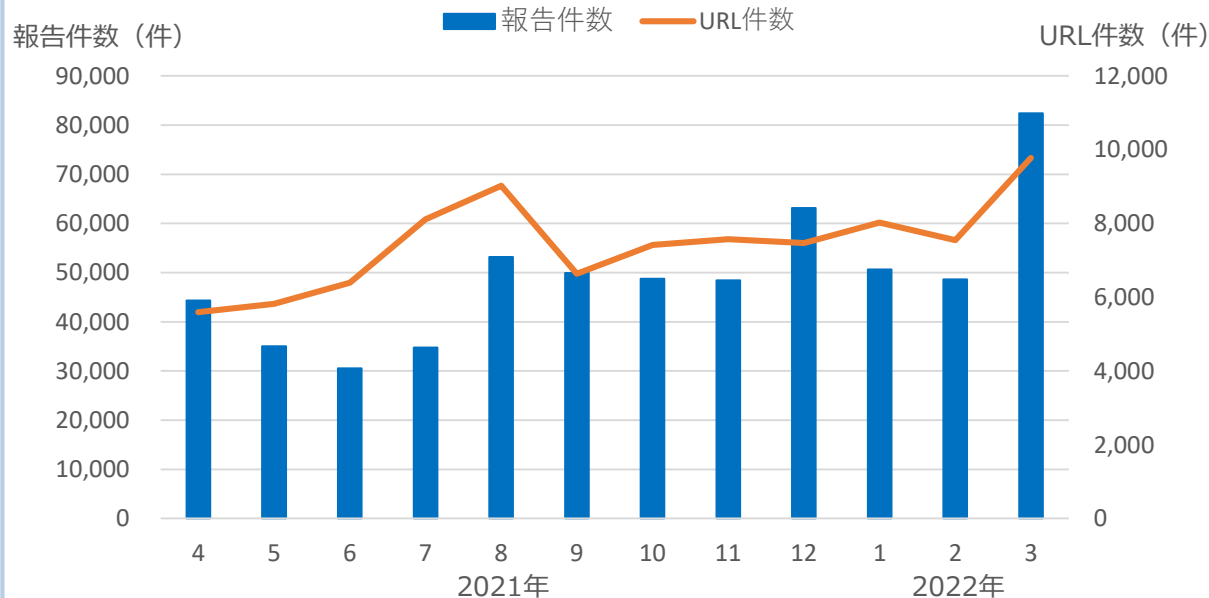
◆ ネットショッピング利用率の増加

▶ 新型コロナウイルス感染拡大を境にネットショッピングの利用率が増加。



◆ フィッシングの増加

▶ フィッシング報告件数、フィッシングサイト件数は、ともに増加傾向。



◆ サプライチェーン複雑化

主要通信機器の世界シェア

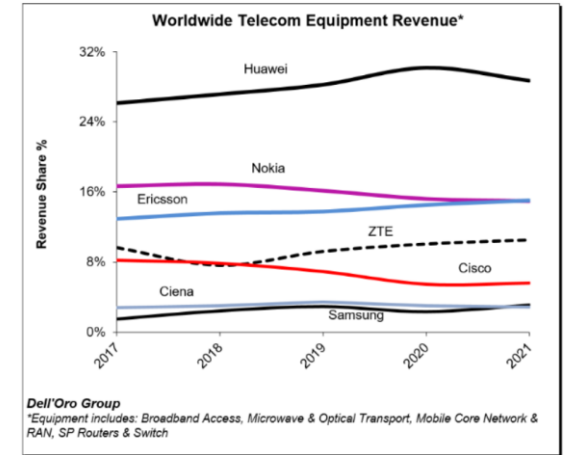
サーバー(2021年2Q)	
HPE/New H3C【米国/中国】	15.7%
デル【米国】	15.6%
インスパイア【中国】	9.4%
レノボ【中国】	7.0%
IBM【米国】	5.0%
その他	47.5%

(データ出所) IDC

スマートフォン(2021年)	
サムスン【韓国】	20.1%
アップル【米国】	17.4%
シャオミ【中国】	14.1%
オッポ【中国】	9.9%
ヴィーヴォ【中国】	9.5%
その他	29.1%

(データ出所) IDC

移動通信インフラ



(データ出所) Dell'Oro Group

◆ 経済社会全体での人材不足・偏在／リテラシーギャップの顕在化

▶ 人材不足感が大きく、IT企業に偏在。

セキュリティ対策に従事する
人材の不足感

90.4% (米12.9%)

(データ出所) NRIセキュア

「企業における情報セキュリティ実態調査2021」

▶ サイバー空間拡大の中、リテラシー浸透が急務。

インターネットの利用時に
不安を感じる人の割合

75%

(データ出所) 総務省

「令和2年通信利用動向調査」

情報処理・通信に携わる人材が
IT企業に所属している割合

72% (米35%)

(データ出所) IPA

「IT人材白書2017」

インターネットや情報に関する倫
理教育を受けたことがある割合

26.0%

(データ出所) IPA

「2021年度情報セキュリティに対する意識調査」

環境変化、国際情勢から見たリスク（２）

◆ 情報セキュリティに関する脅威

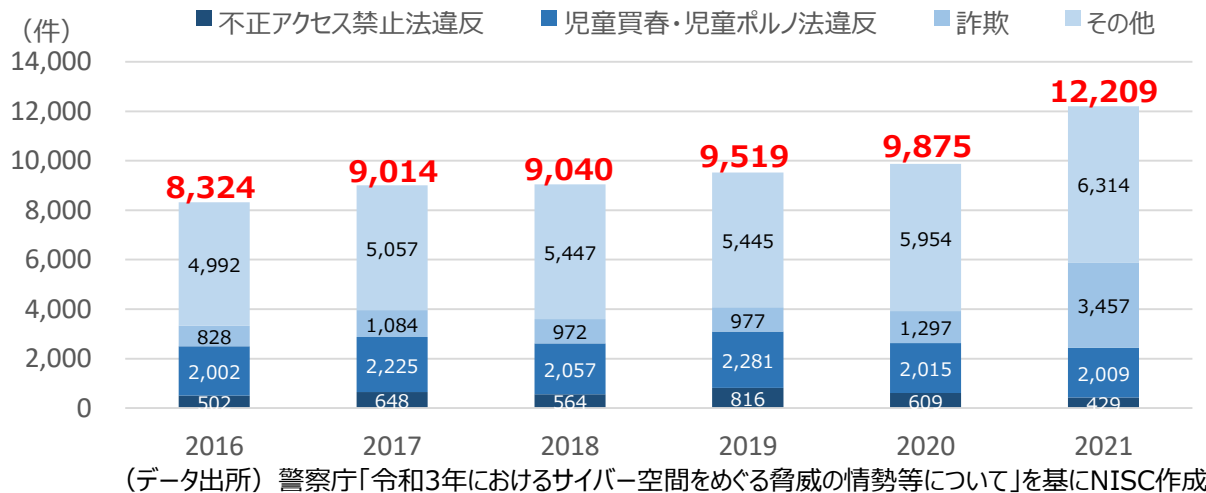
	個人	組織
1位	フィッシングによる個人情報等の詐取	ランサムウェアによる被害
2位	ネット上の誹謗・中傷・デマ	標的型攻撃による機密情報の窃取
3位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	サプライチェーンの弱点を悪用した攻撃
4位	クレジットカード情報の不正利用	テレワーク等のニューノーマルな働き方を狙った攻撃
5位	スマホ決済の不正利用	内部不正による情報漏えい
6位	偽警告によるインターネット詐欺	脆弱性対策情報の公開に伴う悪用増加
7位	不正アプリによるスマートフォン利用者への被害	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
8位	インターネット上のサービスからの個人情報の窃取	ビジネスメール詐欺による金銭被害
9位	インターネットバンキングの不正利用	予期せぬIT基盤の障害に伴う業務停止
10位	インターネット上のサービスへの不正ログイン	不注意による情報漏えい等の被害

- 組織の脅威において、修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)が **新たに7位にランクイン**。

(データ出所) IPA「情報セキュリティ10大脅威2022」を基にNISC作成

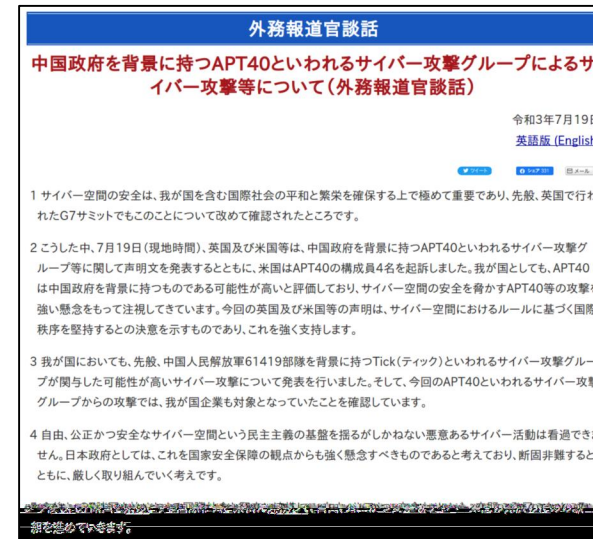
◆ 環境変化をとらえたサイバー攻撃の増加

- サイバー犯罪の検挙件数は増加傾向。2021年中の検挙件数は12,209件で **過去最多**。



◆ サイバー攻撃の組織化、国家の関与が疑われるサイバー攻撃

- 2021年7月、**中国政府**を背景に持つ可能性が高いサイバー攻撃グループや、**中国人民解放軍**を背景に持つサイバー攻撃グループが関与した可能性が高いサイバー攻撃について断固非難するとともに、厳しく取り組んでいく旨の外務報道官談話の発出等がなされている。



(データ出所) 外務報道官談話（令和3年7月19日公表）

国家の関与が疑われるサイバー攻撃

外務報道官談話

米国による北朝鮮のサイバー攻撃に関する発表について（外務報道官談話）

平成29年12月20日
英語版 (English)

ツイートシェア0メール

1 サイバー空間の安全は、我が国を含む国際社会の平和と繁栄を確保する上で極めて重要です。

2 こうした中、12月19日、米国は、本年5月の悪意あるプログラム「ワナクライ」を用いたサイバー攻撃が北朝鮮によるものであるとして、北朝鮮を非難する旨発表しました。

3 我が国は、サイバー分野を含む北朝鮮問題について米国を含む国際社会と緊密に連携してきており、北朝鮮に対する圧力を最大限まで高め、北朝鮮の政策を変えさせるとの観点からも、サイバー空間の安全の確保に向けた強い意思を示す今回の米国の発表を支持するとともに、我が国としても、「ワナクライ」事案の背後に、北朝鮮の関与があったことを非難します。

4 我が国としては、米国を始めとする国際社会と緊密に連携して、自由、公正かつ安全なサイバー空間の創出・発展のための取組を進めていきます。

外務報道官談話

中国政府を背景に持つAPT40といわれるサイバー攻撃グループによるサイバー攻撃等について（外務報道官談話）

令和3年7月19日
英語版 (English)

ツイートシェア0メール

1 サイバー空間の安全は、我が国を含む国際社会の平和と繁栄を確保する上で極めて重要であり、先般、英国で行われたG7サミットでもこのことについて改めて確認されたところです。

2 こうした中、7月19日（現地時間）、英国及び米国等は、中国政府を背景に持つAPT40といわれるサイバー攻撃グループ等に関して声明文を発表するとともに、米国はAPT40の構成員4名を起訴しました。我が国としても、APT40は中国政府を背景に持つものである可能性が高いと評価しており、サイバー空間の安全を脅かすAPT40等の攻撃を強い懸念をもって注視してきています。今回の英国及び米国等の声明は、サイバー空間におけるルールに基づく国際秩序を堅持するとの決意を示すものであり、これを強く支持します。

3 我が国においても、先般、中国人民解放軍61419部隊を背景に持つTick（ティック）といわれるサイバー攻撃グループが関与した可能性が高いサイバー攻撃について発表を行いました。そして、今回のAPT40といわれるサイバー攻撃グループからの攻撃では、我が国企業も対象となっていたことを確認しています。

4 自由、公正かつ安全なサイバー空間という民主主義の基盤を揺るがしかねない悪意あるサイバー活動は看過できません。日本政府としては、これを国家安全保障の観点からも強く懸念すべきものであると考えており、断固非難するとともに、厳しく取り組んでいく考えです。

※ 上記のほか、2018年12月には、「中国を拠点とするAPT10といわれるグループによるサイバー攻撃について」（外務報道官談話）を公表。

MEMO

警察のアトリビューションにより国家レベルの関与を明らかにしたサイバー攻撃事案

1 レンタルサーバ不正契約事件被疑者の検挙

中国共産党員の男（30代）は、平成28年9月から平成29年4月までの間、合計5回にわたり、住所、氏名等の情報を偽って日本のレンタルサーバの契約に必要な会員登録を行った。警視庁公安部は、令和3年4月、同男を私電磁的記録不正作出罪・同供用罪で検挙した。

2 一連のサイバー攻撃に関与した背景組織の特定

本事件の捜査を通じ、警察では、同男が不正に契約したレンタルサーバが宇宙航空研究開発機構（JAXA）等に対するサイバー攻撃に悪用されたことを把握するとともに、同攻撃の実態解明の過程で、同一の攻撃者が関与している可能性が高いサイバー攻撃が約200の国内企業等に対して実行されたことを把握した。

本事件被疑者・関係者の供述をはじめ数多くの証拠を積み上げた結果、これらのサイバー攻撃がTickと呼ばれるサイバー攻撃集団によって実行されたものであり、このTickの背景組織として山東省青島市を拠点とする中国人民解放軍第61419部隊が関与している可能性が高いと結論付けるに至った。

3 被害企業等に対する注意喚起

警察では、これらのサイバー攻撃を認知後、被害企業等に対し、速やかに不正プログラムへの感染可能性や有効な対応策について個別に情報提供を実施した^{注1}。

また、一連のサイバー攻撃は、日本製ソフトウェアのぜい弱性が悪用されたゼロデイ攻撃^{注2}であったことから、このソフトウェアの開発企業と協力し、ぜい弱性の存在と有効な対応策について広く周知した。

[出典]令和3年警察白書

APT40に対してNISC・警察庁による注意喚起を実施

NISC 内閣府サイバーセキュリティセンター
National Center of Incident Coordination and Response for Cybersecurity

警察庁
National Police Agency

2021年7月19日

中国政府を背景に持つAPT40といわれるサイバー攻撃グループによるサイバー攻撃等について（注意喚起）

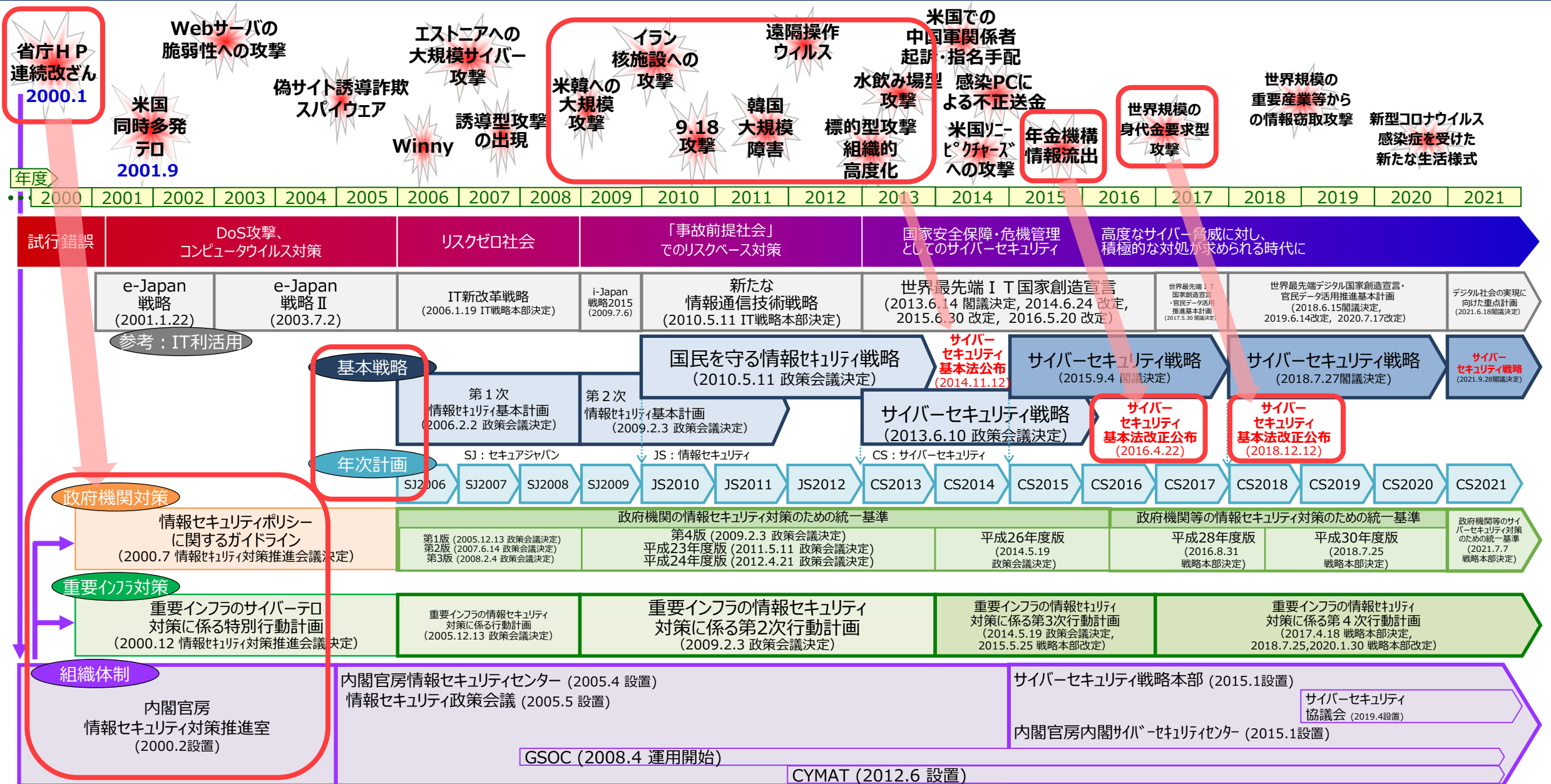
令和3年7月19日（現地時間）、英国及び米国等は、中国政府を背景に持つAPT40といわれるサイバー攻撃グループ等に関して、声明文を発表しました。

我が国政府としても、サイバー空間の安全を脅かすAPT40等の攻撃を強い懸念を持って注視してきており、7月19日、こうした悪意あるサイバー活動を断固非難するとともに、厳しく取り組んでいく旨の外務報道官談話を発出しました。
（中国政府を背景に持つAPT40といわれるサイバー攻撃グループによるサイバー攻撃等について（外務報道官談話）
https://www.mofa.go.jp/mofaj/press/danwa/page6_000583.html

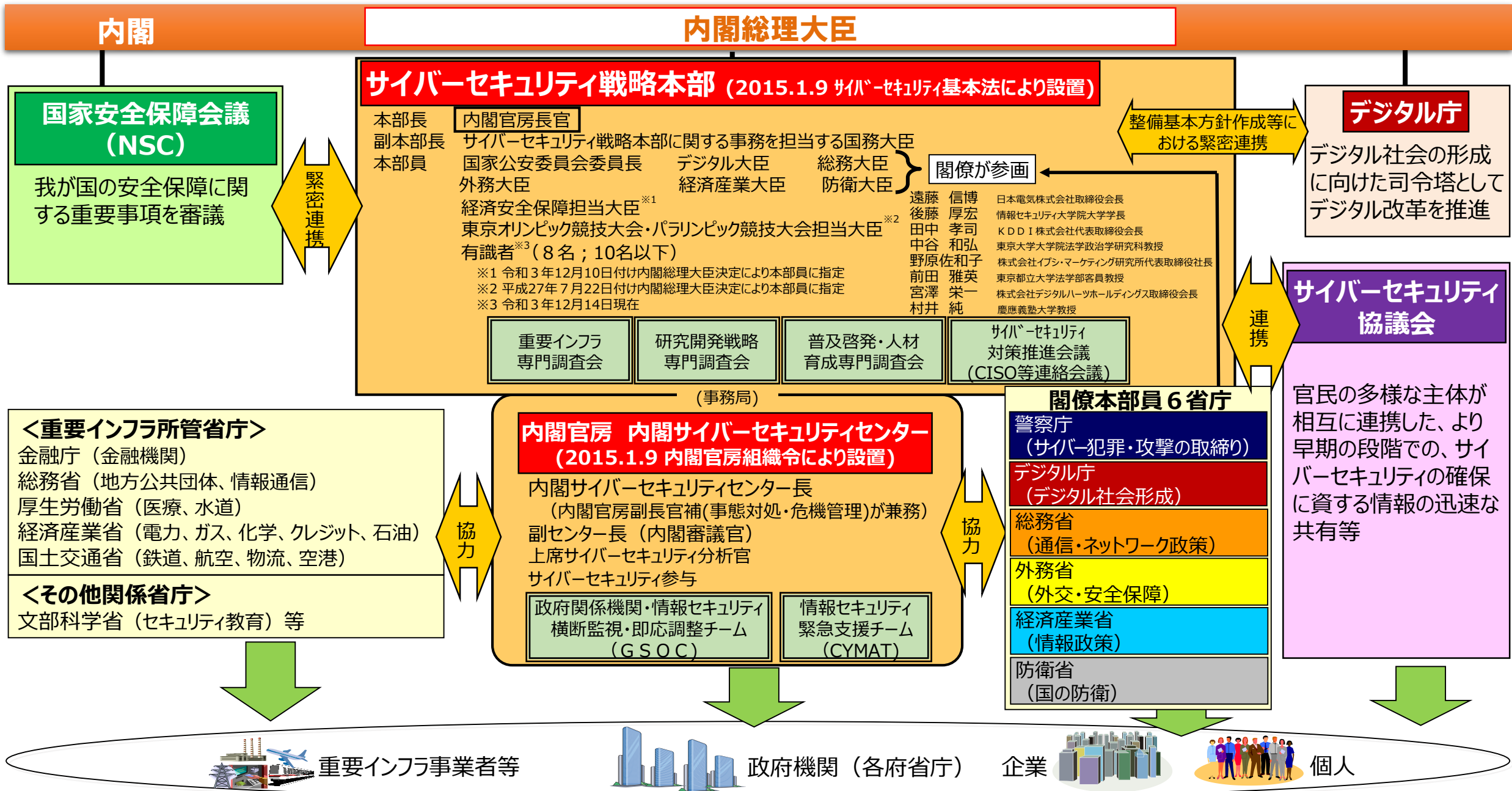
今回のAPT40といわれるサイバー攻撃グループによるサイバー攻撃等では、我が国企業も対象となっていたことを確認しているところであり、内閣サイバーセキュリティセンターや警察では、引き続き国内外の関係機関と連携し、被害の未然防止及び拡大防止に向けて情報収集や対策等を進めてまいります。

こうしたサイバー攻撃にはさまざまな手法、手口がありますが、日頃から、不審なメールや添付ファイルは開かない、OSやプログラムのパッチやアップデートを可及的速やかに設定する等の基本的な留意事項を守りつつ、対象に応じた適切なサイバーセキュリティ対策を講じてください。また、実際に情報流出等の被害が発生していなかったとしても、不審な動きを検知した場合は、速やかに所管省庁、セキュリティ関係機関に対して連絡していただくとともに、警察にもご相談ください。

サイバーセキュリティ政策の経緯



我が国におけるサイバーセキュリティ政策推進体制



サイバーセキュリティ戦略の課題と方向性

2021年9月28日閣議決定

2020年代を迎えた日本を取り巻く時代認識：「ニューノーマル」とデジタル社会の到来

デジタル経済の浸透、デジタル改革の推進

新型コロナウイルスの影響・経験
テレワーク、オンライン教育等の進展

厳しさを増す
安全保障環境

SDG s への
デジタル技術の貢献期待

東京オリンピック・パラリンピックに
向けて行ってきた取組

サイバー空間をとりまく課題認識：国民全体のサイバー空間への参画

サイバー空間は、国民全体等あらゆる主体が参画し公共空間化
サイバー・フィジカルの垣根を超えた各主体の相互関連・連鎖の深化
攻撃者に狙われ得る弱点にも

地政学的緊張を反映
国家間競争の場に
安全保障上の課題にも

不適切な利用は
国家分断、人権の阻害へ

官民の取組の
活用

あらゆる主体にとってサイバーセキュリティの確保は自らの問題に
5つの基本原則※は堅持

「Cybersecurity for All」

～誰も取り残さないサイバーセキュリティ～

デジタルトランスフォーメーション（DX）
とサイバーセキュリティの同時推進

安全保障の観点からの取組強化

公共空間化と相互関連・連鎖が進展する
サイバー空間全体を俯瞰した
安全・安心の確保

「自由、公正かつ安全なサイバー空間」の確保

※情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携

新しい「サイバーセキュリティ戦略」のポイント（新旧比較）

2021年9月28日閣議決定

- 基本法における3つの目的（※）を達成するための施策について、「Cybersecurity for All～誰も取り残さないサイバーセキュリティ～」という大きな方向性を示しつつ、デジタル改革やDXの進展に伴う課題、経済安全保障の懸念、国家の関与が疑われる攻撃の脅威の高まり等**新たな脅威認識**の下、**国民目線**、**公助の取組強化**の観点から新しい戦略を策定。

（※） **経済社会の活力の向上及び持続的発展** **国民が安全で安心して暮らせる社会の実現** **国際社会の平和・安定及び我が国の安全保障への寄与**

2018戦略

1 社会のデジタル化への対応

- 経営層、サプライチェーン対策

2 重点領域の拡大

- 政府機関、重要インフラ事業者

3 サイバー防御体制の強化

- 多様な主体間の情報共有・連携の推進（サイバーセキュリティ協議会の設立）
- 民間の参加・連携・協働の支援

4 サイバー抑止力の向上、国際連携の強化

- 防御力・抑止力・状況把握力の強化（自衛隊等関係機関の強化）
- 対外発信（脅威対象国、連携強化国は明記せず）

5 人材育成等

- 人材：戦略マネジメント層の育成
- 研究：実践的開発の推進

2021戦略

- 経営層、サプライチェーン対策
- 子ども・高齢者のリテラシー対策

- 政府機関、重要インフラ事業者
- サイバー関連事業者（主にクラウドサービス）
- 知的財産、個人情報を扱う事業者

- 国主導による重大サイバー事案への対処（ナショナルサート機能の強化※¹、警察庁サイバー局設置等）
- 経済安全保障（ITインフラの信頼性確保）

- 外交安保上の優先度向上
- 防御力・抑止力・状況把握力の強化（妨げる能力の活用、外交的手段、刑事訴追）
- 対外発信（脅威対象としての中※²露北、連携強化国として米豪印、ASEANの明記）

※² JAXA等に対する攻撃に関し言及

- 人材：戦略マネジメント層の育成（「プラスセキュリティ知識」※³の補充）
高度専門人材の育成・確保
- 研究：実践的開発、AI、量子の対応具体化

※³ セキュリティ専門家と協働するために、自らの業務にプラスして習得すべき知識

横断的施策

DXとサイバーセキュリティ
の同時推進

公共空間化と相互関連・連鎖が進展する
サイバー空間全体を俯瞰した
安全・安心の確保

安全保障の観点からの
取組強化

● 上記の推進に向け、横断的・中長期的な視点で、研究開発や人材育成、普及啓発に取り組む。

1. 研究開発の推進

産学官エコシステム構築とともに、それを基盤とした実践的な研究開発推進。
中長期的な技術トレンドも視野に対応。

(2)実践的な研究開発の推進

- ① サプライチェーンリスクへの対応
- ② 国内産業の育成・発展
- ③ 攻撃把握・分析・共有基盤
- ④ 暗号等の研究の推進

(1)国際競争力の強化 産学官エコシステムの構築

- ・研究・産学官連携振興施策の活用
- ・研究環境の充実 等

(3)中長期的な技術トレンド を視野に入れた対応

- ① AI技術の進展
AI for Security
Security for AI
- ② 量子技術の進展
耐量子計算機暗号の検討
量子通信・暗号

2. 人材の確保、育成、活躍促進

「質」・「量」両面での官民の取組を一層継続・深化させつつ、環境変化に
対応した取組の重点化。官民を行き来しキャリアを積める環境整備も。

(1)DX with Cybersecurity の推進

- ・「プラス・セキュリティ」知識を補充
できる環境整備
- ・機能構築・人材流動に関する
プラクティス普及 等
(xSIRT、副業・兼業等)

(2)巧妙化・複雑化する 脅威への対処

- ・人材育成プログラムの強化
SecHack365 / CYDER / enPiT
ICSCoE中核人材育成プログラム 等
- ・人材育成共通基盤の構築
産学への開放
- ・資格制度活用に向けた取組 等

優秀な人材が民間、自治体、政府を行き来しながらキャリアを積める環境の整備

(3)政府機関における取組 外部高度人材活用の仕組み強化 「デジタル区分」合格者の積極採用、研修の充実・強化 等

3. 全員参加による協働、普及啓発

デジタル化推進を踏まえ、アクションプランの推進・改善、高齢者への対応を含め見直しの検討。

- サイバーセキュリティ戦略において、各年度ごとに取組状況を年次報告として取りまとめ、次年度の年次計画に反映することとしていることを踏まえて策定するもの。
- 従来の構成の冒頭にエグゼクティブ・サマリーを設け、サイバー空間をめぐる課題と対応の方向性を明らかにし、発信力を強化する観点から、昨今の国際情勢等を踏まえた課題と、戦略本部として特に強力に取り組む施策を明記。

1. サイバー空間を巡る主な情勢の変化と昨今の状況

- 新型コロナウイルス感染症による「ニューノーマル」の拡大
 - デジタルトランスフォーメーション（DX）の進展
 - 国際情勢の変化によるサイバーリスクの増大
- 
- 国内でも多様なインシデントが発生
 - ✓ ランサムウェアによる被害拡大
 - ✓ Emotetによる被害拡大

2. 情勢の変化に伴い顕在化している政策課題

- (1) サイバー空間上における脅威の高まりに対応するための**インシデントの未然防止**
- (2) 「公共空間化」によるリスクの広がりに対応するための**地域・中小企業等のセキュリティ強化・支援、サイバー犯罪への対応強化**による安全・安心の確保
- (3) 厳しさを増す安全保障環境の中での**国際協力・連携の強化**

3. 「自由、公正かつ安全なサイバー空間」の実現のために特に強力に取り組む施策

1) 官民連携のオールジャパンの推進体制（ナショナルサート機能の強化）

インシデントの未然防止のための、情報収集・分析力の向上や官民情報共有体制の強化

2) 重要インフラ事業者を始めとする民間部門におけるサイバーセキュリティの強化

「重要インフラのサイバーセキュリティに係る行動計画」を踏まえた取組の推進、サイバーインフラの強靱性の確保 等

3) サイバー・フィジカル空間の融合に対応したサイバーセキュリティ対策

ソフトウェアの脆弱性管理等のためのソフトウェア部品表（SBOM※）の普及に向けた取組の推進 等

※SBOM: Software Bill Of Materials

4) 地域・中小企業のサイバーセキュリティ対策

経営者の意識改革、地域で共助の取組を推進するセキュリティ・コミュニティ（地域SECURITY）の活動促進、中小企業に対する「サイバーセキュリティお助け隊」の普及

5) サイバー警察局・サイバー特別捜査隊の新設による官民連携・国際連携の推進

深刻化するサイバー空間の脅威に適切に対処し、安全・安心を確保していくための取組

6) インド太平洋地域における能力構築支援の推進

ASEAN諸国の政府機関に対する演習等を通じたインド太平洋地域における能力構築支援の取組の一層の推進

重要インフラのサイバーセキュリティに係る行動計画（概要）

2022年6月17日サイバーセキュリティ戦略本部決定

- 安全で安心な社会の実現には、官民の緊密な連携による重要インフラのサイバーセキュリティの確保が必要であり、基本的な枠組みとして、**政府と重要インフラ事業者等との共通の行動計画**※を推進してきた。

※ 「重要インフラの情報セキュリティ対策に係る第4次行動計画」（平成29年4月18日サイバーセキュリティ戦略本部決定）

- 重要インフラを取り巻く脅威は年々高度化・巧妙化している中で、昨年のサイバーセキュリティ戦略（令和3年9月28日閣議決定）の策定を踏まえ、**新たな行動計画を策定**する。

◆ 第4次行動計画における有効な取組は継続

◆ 組織統治の一部としてサイバーセキュリティを組み入れ、組織全体で対応

◆ 重要インフラを取り巻く脅威の変化に対応するため、将来の環境変化を先取りし、サプライチェーンを含めてリスクを明確化し対応

重要インフラ(全14分野)

情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット、石油

第4次行動計画

新たな行動計画(案)

障害対応体制の強化

- 経営層に対し、サイバーセキュリティに関する意識を高めるよう働きかけ
- 事業継続計画の整備とそれを実行するための組織体制の構築

- 経営層、CTEC、業務責任者層、システム担当等、組織全体での取組となるよう、組織統治の一部としてサイバーセキュリティを組み入れる。必要な観点として、経営層の重要インフラサービス障害等に対する責任等を明記
- 重要インフラサービスを提供するために必要なサプライチェーン等に関わる事業者が、サイバーセキュリティ基本法に基づき、サイバーセキュリティの確保に努める責任を有する旨を明記し、組織の壁を越えたサプライチェーン全体で障害対応能力を向上

安全基準等の整備・浸透

- 分野横断的に必要な対策を共通指針として策定
- 事業者の取組についてのアンケート調査・ヒアリング

- 組織統治、サプライチェーン等の観点から共通指針を改定
- 事業者における経営層のリーダーシップ、セキュリティ対策等の取組状況をより正確に把握し、取組の継続的な改善を促進

情報共有体制の強化

- 多様な連絡形態による情報共有
- 共有情報の明確化

- 重要インフラ事業者等の自主的な取組の活性化を前提とした共助の推進
- ナショナルサートの枠組みの強化の検討との整合性保持

リスクマネジメントの活用

- リスク評価の推進

- 経営層による自組織の特性の把握、サプライチェーン・リスクを含めたリスクの明確化等により自組織に適した防護対策の実現を促進

防護基盤の強化

- 官民が連携して行う演習等の実施

- 障害対応体制の有効性検証としての分野横断的演習の推進
- 警察、デジタル庁との連携強化

現下の情勢を踏まえた注意喚起の実施

- 昨今の情勢を踏まえたサイバー攻撃事案の潜在的なリスクが高まっており、政府から、2022年2月23日、3月1日、3月24日と、立て続けに注意喚起を発出。

令和4年3月24日

経済産業省

総務省

警察庁

内閣官房内閣サイバーセキュリティセンター

現下の情勢を踏まえたサイバーセキュリティ対策の強化について（注意喚起）

昨今のサイバー攻撃事案のリスクの高まりを踏まえ、政府においては、2月23日に「昨今の情勢を踏まえたサイバーセキュリティ対策の強化について（※1）」、3月1日に「サイバーセキュリティ対策の強化について（※2）」注意喚起を行っております。

その後も、国内では、ランサムウェアによる攻撃をはじめとするサイバー攻撃事案の報告が続いており、また、エモテットと呼ばれるマルウェアの増加も見られるところです。また、米国では、3月21日に、バイデン大統領が、国内の重要インフラ事業者等に対して、ロシアが潜在的なサイバー攻撃の選択肢を模索しており警戒を呼びかける声明を発表するとともに、企業等に対してサイバーセキュリティ対策を強化する具体策を提示しています。

このような現下の情勢を踏まえ、政府機関や重要インフラ事業者をはじめとする各企業・団体等においては、組織幹部のリーダーシップの下、サイバー攻撃の脅威に対する認識を深めるとともに、上記の**2月23日及び3月1日の注意喚起にある対策（①リスク低減のための措置、②インシデントの早期検知、③インシデント発生時の適切な対処・回復）の徹底**をあらためてお願いいたします。また、ランサムウェアやエモテットについては、これまで専門機関等において公表している情報・サイトを確認の上、対応を講じるようお願いいたします。あわせて、不審な動き等を検知した場合は、速やかに所管省庁、セキュリティ関係機関に対して情報提供いただくとともに、警察にもご相談ください。

（以下、参考URL（略））

【参考】

- ※1）**2月23日、経済産業省より、「昨今の情勢を踏まえたサイバーセキュリティ対策の強化」（注意喚起）を発出。**（各企業・団体に対して、経営者のリーダーシップの下、脅威への認識を深め、リスク低減のための措置、インシデントの早期検知、インシデント発生時の適切な対処・回復を要請。）
- ※2）**3月1日、トヨタ事案を踏まえ、経済産業省、金融庁、総務省、厚生労働省、国土交通省、警察庁、NISCの連名により、「サイバーセキュリティ対策の強化」（注意喚起）を発出。**（政府機関や重要インフラ事業者を初めとする各企業・団体等に対策の強化を要請。）

参考) 米国・合同アドバイザリーの構成要素の一例 (APT40のケース) 仮訳

- 米国では、CISA(防御)、ODNI/NSA(安保)、FBI(警察)で構成される“Cyber Unified Coordination Group(UCG)”が連携し、合同アドバイザリー(脅威評価と技術情報から構成される注意喚起文書)を発出。

中華人民共和国国家安全部海南省国国家安全保衛部に関連する、起訴されたAPT40アクターの戦術、技術、手順

概要

この共同サイバーセキュリティ・アドバイザリーは、米連邦捜査局(FBI)とサイバーセキュリティ・インフラセキュリティ局(CISA)が作成したもので、オープンソースの報道でAPT40として知られている中国のAPTグループに関する情報を提供します。このアドバイザリーは、APT40の戦術、技術、手順(TTP)とセキュリティ侵害インジケーター(IoC)を提供して、サイバーセキュリティの実務者がAPT40の侵入と確立された拠点を特定し、修正するのに役立ちます。

APT40-別名BRONZE MOHAWK、FEVERDREAM、G0065、ガドリニウム、GreenCrash、HELLSING、クリプトナイトパンダ、リバイアサン、MUDCARP、Periscope、Temp.Periscope、およびTemp.Jumperは、中国(PRC)の海南省海口市にあり、少なくとも2009年から活動しています。APT40は、米国、カナダ、欧州、中東、南シナ海地域の生物医学、ロボット工学、海洋研究、中国の「一帯一路構想」に含まれる産業など、幅広い産業分野の政府機関、企業、大学を対象としています。

2021年7月19日、米国司法省は、4人のAPT40サイバーアクターがフロントカンパニーである海南仙盾技術開発会社(海南仙盾)を通じて不正なコンピュータ・ネットワーク利用(CNE)活動を行ったとして起訴しました。海南省の職員であるWu Shurong氏は、中国国家安全省(MSS)の海南省国家安全保衛部(HSSD)の情報官であるDing Xiaoyang氏、Zhu Yunmin氏、Cheng Qingmin氏と協力してCNEを実施しました。呉氏のCNE活動は、米国内外の企業や組織、複数の外国政府から企業秘密、知的財産、その他の価値の高い情報を盗み出す結果となりました。これらのMSS関連のアクターは、学界、航空宇宙・航空、生物医学、防衛産業基盤、教育、政府、医療、製造、海事、研究機関、運輸(鉄道および海運)などの産業の被害者を対象としています。(中略)

技術詳細

APT40[G0065]では、さまざまな戦術と手法、およびカスタムでオープンソースのマルウェアの大規模なライブラリを使用しています。これらのマルウェアの多くは、他の複数の疑わしい中国人グループと共有されています。これにより、ユーザーおよび管理者の資格情報による初期アクセスを確立し、ネットワーク内で一度横方向に移動できるようにし、データを抽出するために価値の高い資産を特定できます。これらの戦術と手法の詳細を表1に示します。注:このアクティビティを容易にするために使用されるドメイン、ファイル名、およびマルウェアMD5ハッシュ値のリストについては、付録を参照してください。

表1: APT40 ATT&CKの戦術とテクニック(記載省略)

防御策

ネットワークの深層防御

適切なネットワーク防御と情報セキュリティのベストプラクティスの遵守は、脅威の軽減とリスクの軽減に役立ちます。以下のガイダンスは、組織がネットワーク防御手順を策定するのに役立つ可能性があります。

パッチおよび脆弱性管理

ベンダーが提供し、検証済みのパッチをすべてのシステムにインストールして、重大な脆弱性に対処します。優先順位は、インターネットに接続されたサーバおよびソフトウェア処理インターネットデータ(Webブラウザ、ブラウザプラグイン、ドキュメントリーダーなど)のタイムリーなパッチ適用です。(以下略)

認証情報の保護

クレデンシャル要件を強化し、パスワードを定期的に変更し、マルチファクタ認証を実装して、個々のアカウント、特にWebメールとVPNアクセス、および重要なシステムにアクセスするアカウントを保護します。複数のアカウントのパスワードは再使用しないでください。(以下略)

ネットワークの衛生および監視

インターネットにアクセス可能なアプリケーションを積極的にスキャンして監視し、不正なアクセス、変更、異常なアクティビティがないかどうかを確認します。(以下略)

付録: APT40のIoC

APT40は、次のドメイン、ファイル名、およびマルウェアMD5ハッシュ値を使用して、2009~2018の間のこのCSAで概説されているCNEアクティビティを容易にしました。(以下ドメイン及びハッシュ値が列挙。記載省略)



: 脅威・情勢認識



: 攻撃手法分析



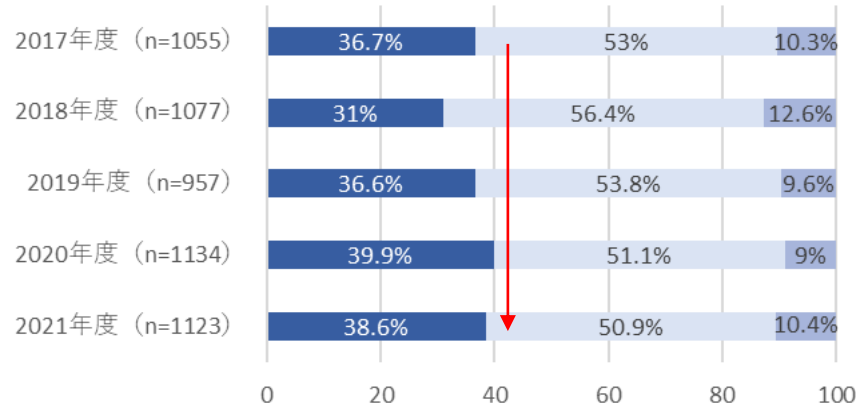
: 防御策の周知



: IoC情報

■ セキュリティ対策に関し、経営層の関与は大きく進展しておらず、他国と比べてもその水準は低い。

■ 日本企業におけるセキュリティへの経営層の関与度合い



■ 経営層は、セキュリティリスクを経営課題のひとつと認識しており、セキュリティリスクや重大なセキュリティ対策については、経営会議等で審議・決定される

- 経営層は、セキュリティリスクや重大なセキュリティ対策の重要性を認識しているが、取組みは主にIT部門などに任せ経営会議で議論されない
- 経営層は、セキュリティリスクおよび対策について重要性を認識しておらず、ほとんど会話することがない

[出典] (一社) 日本情報システムユーザー協会 各年度の「企業IT動向調査報告書」よりNISC作成

■ 日本企業におけるスキル・マトリックスへの記述状況

- ・ 株式時価総額トップ100企業のうち、スキル・マトリックスを開示している企業は50社。
- ・ 上記50社のうち、「セキュリティ」に関する項目を設けていた企業は6% (3社)。

[出典] コーン・フェリー・ジャパン「スキル・マトリックスの開示状況」(2021年6月) よりNISC確認

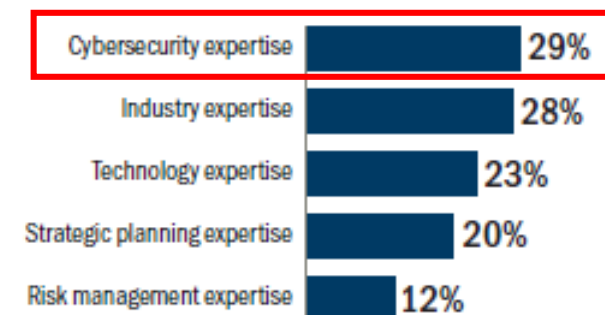
cf. 米国の動向

■ 自社のサイバーセキュリティ状況について取締役会に報告する役職



[出典] “NACD Public Company Governance Survey 2019-20” (2019.12)

■ 強化する必要がある専門知識の領域 (経営陣)



[出典] “NACD Public Company Governance Survey 2016-17”(2016.11)

対策実施と経営層の指示との関係性

- セキュリティ対策実施のきっかけはインシデント事例に基づくケースが多く、米国と比較して、経営層のトップダウン指示に基づくケースは低い。
- 自社のセキュリティに対する課題認識について、「経営層・役員」と「部長」の間で差異がみられる。

■ 直近1年に実施したセキュリティ対策の実施のきっかけや理由

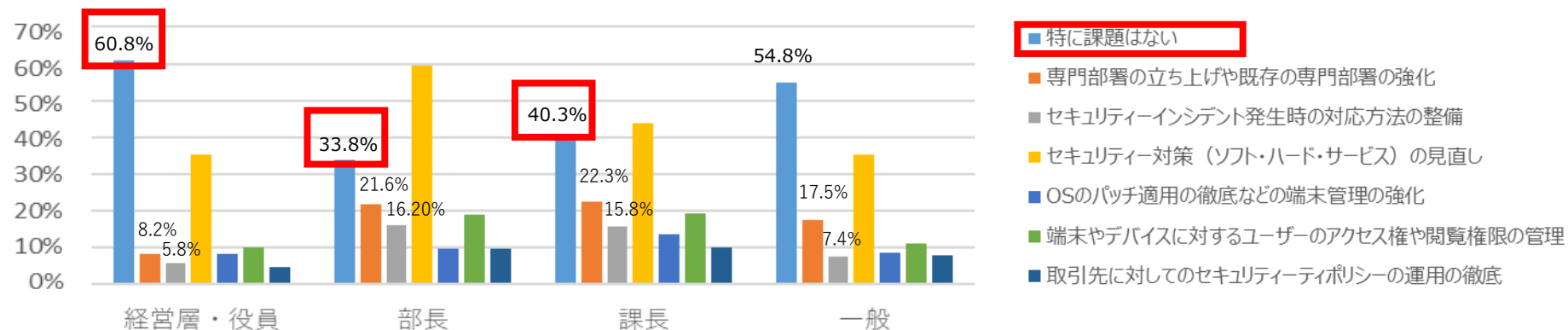
	日本	米国
1位	27.6% 他社でのセキュリティインシデント事例	54.8% 経営層のトップダウン指示
2位	25.6% 自社でのセキュリティインシデント事例	25.0% 他社でのセキュリティインシデント事例
3位	21.6% 経営層のトップダウン指示	24.5% 株主や取引先からの要請

※ 左記以外の選択肢：

- ・監督省庁からのセキュリティ対策強化の要請（自治体からの要請を含む）
- ・関連法規の改定（具体的な要請内容を記載）
- ・持株会社や親会社からの要請
- ・競合他社の実施状況との比較
- ・外部監査・第三者評価の結果
- ・内部監査・内部有識者からの指摘
- ・COVID-19に伴うテレワーク対応
- ・東京2020大会（オリンピック・パラリンピック）に伴う対応
- ・DX化推進に伴う対応
- ・その他（具体的に記載）
- ・わからない

[出典] NRIセキュアテクノロジーズ㈱「NRI Secure Insight 2021」（2022年2月）

■ 自社におけるセキュリティインシデントに対する課題（役職別）

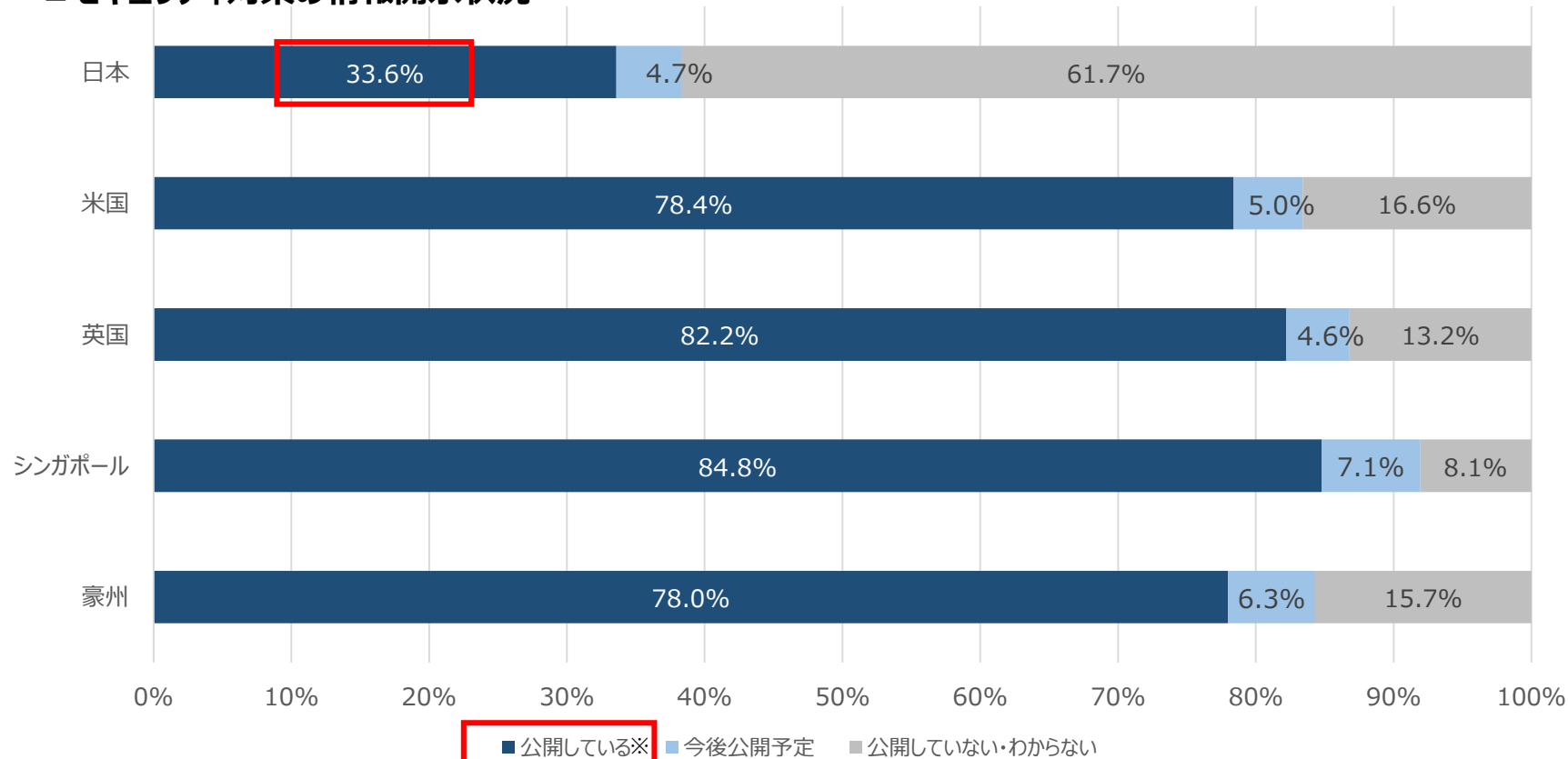


[出典] NTTビジネスソリューションズ(株)「サプライチェーン攻撃に関する市場調査レポート」（2022年5月）よりNISC作成 16

投資家の認識①（情報開示）

■ セキュリティ対策の情報開示も他国と比べて進んでおらず、投資家もリスクや対策状況を認識しづらい状況。

■ セキュリティ対策の情報開示状況



[出典] NRIセキュアテクノロジーズ㈱「企業における情報セキュリティ実態調査 2018」(2018年7月)

※「企業のWebサイトの情報セキュリティに特化したページ（情報セキュリティ報告書等）で公開している」
「企業のWebサイトの情報セキュリティ以外のページ（CSR、年次報告書等）で公開している」
「業界団体やISAC等のコミュニティ内で公開・共有している」
「講演会やセミナー等で公開している」

機関投資家による投資先企業のサイバーセキュリティ対策状況の確認について

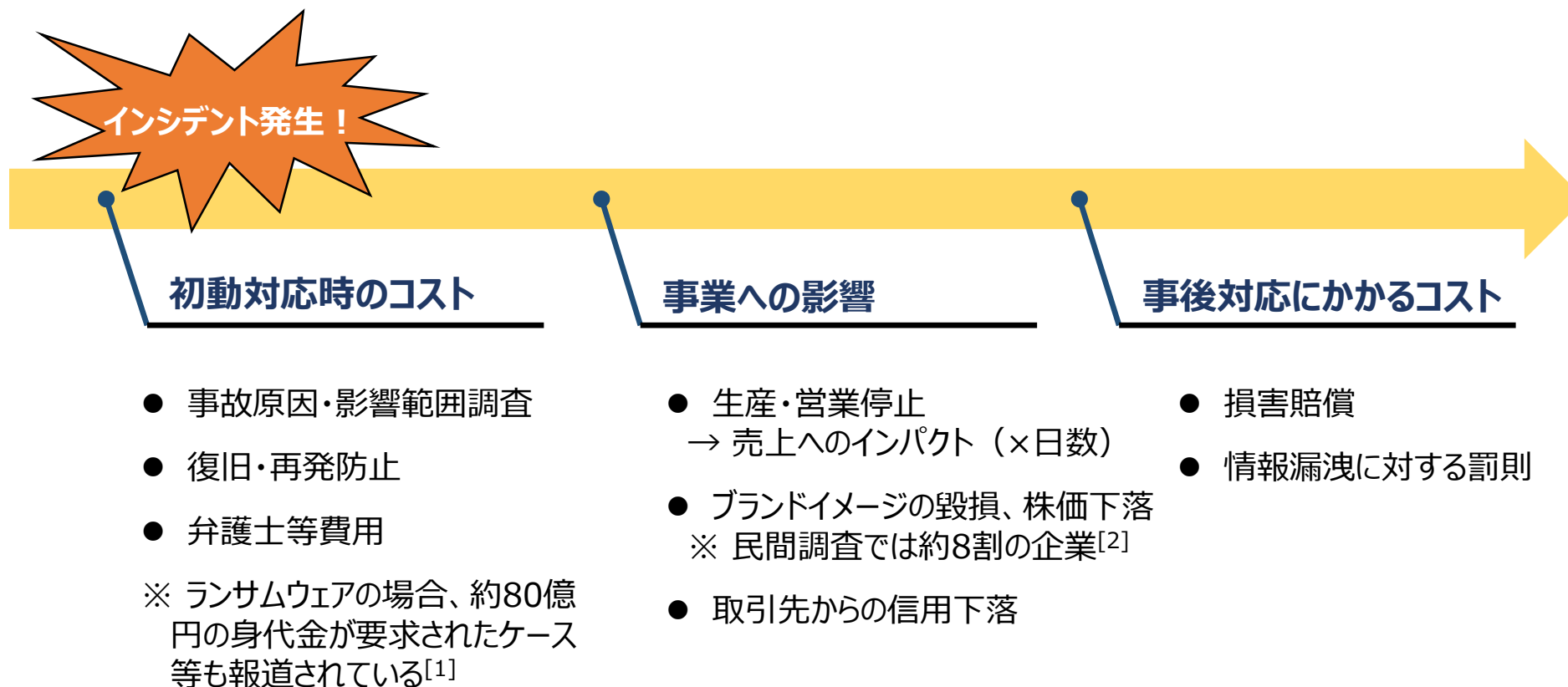
- ✓ セキュリティ体制は機能していることが重要。現場と経営陣が円滑につながっているかを確認したい。
- ✓ 扱う情報が多い業種・業態のリスクは高いと考える。データの流出が企業の存続に関わるようなケースでは詳細に確認する。
- ✓ 開示情報のエビデンスは重視していない。エビデンスがあってもリスクはゼロにならない。プライバシーマークやISO認証などは若干の安心材料だが、体制や想定リスクに関する質問に対し、クリアな情報が提示されることが重要。
- ✓ 事故発生の可能性はゼロにならないので、リカバリーの体制が取られているのかを含めた開示を期待。
- ✓ サイバーセキュリティの世界は、人権デューデリジェンスに近い捕捉の難しさがあると感じている。PDCAを通じたレベルアップを前提に、基準や取組事項をまとめた行動計画を普及させるべきではないか。

今後参考となりそうなポイント（機関投資家等によるDXやリスク管理等に関する評価方法について）

- ✓ 「気候関連財務情報開示タスクフォース（TCFD）」が「ガバナンス」、「戦略」、「リスク管理」、「指標と目標」の4つの柱に関して開示のプロトタイプを示している。投資家はこうした動きになじみはじめており、他のリスクに関しても開示のプロトタイプとして、わかりやすい開示を求める動きが出てくる可能性がある。
- ✓ 法律で開示が求められている情報の内容は各社とも似通っており、あまり読むことはない。自社にとって致命的なリスクをメリハリをもって示すことが重要。

投資家の認識②（経営インパクトに関する認知）

- 経営へのインパクト（金額）について、試算を行う動きもあるが、実際に被害を受けた企業の影響金額が会計上明らかではないため、実際の被害金額等に基づいた試算は国内ではみられない。
- このため、経営層や投資家等が、個別のサイバーセキュリティ対策の費用対効果やサイバーセキュリティに関する経営上のリスクを認識しづらい状況にある。



[1] “REvil gang asks for \$70 million to decrypt systems locked in Kaseya attack” (2021年7月4日)
<https://www.bleepingcomputer.com/news/security/revil-ransomware-asks-70-million-to-decrypt-all-kaseya-attack-victims/>

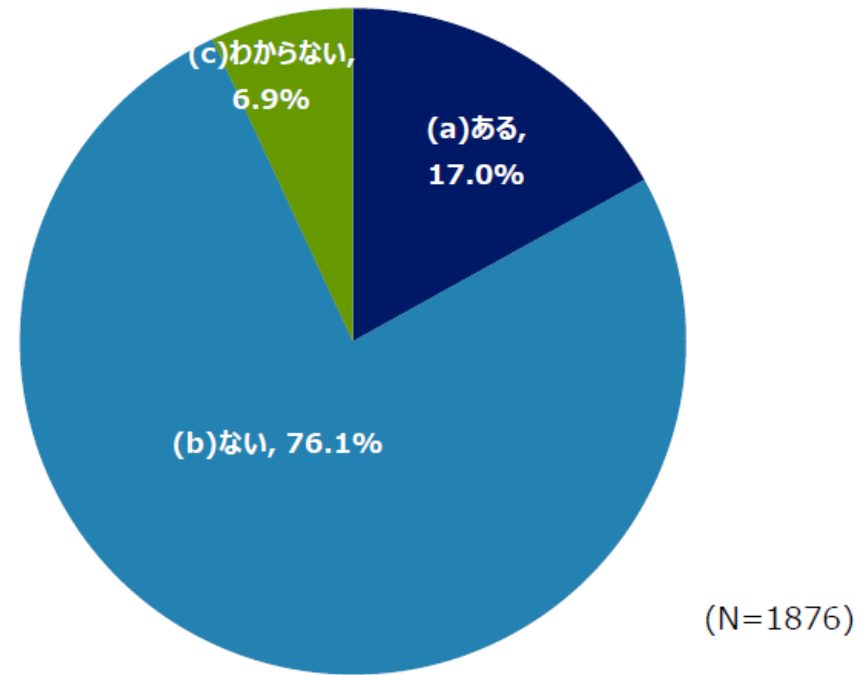
[2] (株)サイバーセキュリティクラウド プレスリリース (2022年2月) <https://www.cscloud.co.jp/news/press/202202174115/>

[全体項目] JNSA「インシデント損害額調査レポート2021」（2021年8月）等よりNISC作成

- 取引先企業がサイバー攻撃の被害を受け、自社に影響を及ぼす事案も一般的になりつつある。

取引先等を経由したサイバー攻撃被害の経験

- 過去に取引先等がサイバー攻撃の被害を受け、それが貴社に及んだ経験がありますか（仕入・外注・委託先等の取引先）



- セキュリティはコストではなく投資であると位置づけ、経営者がリーダーシップを取ってセキュリティ対策を推進していくことが重要であることを示したガイドライン。（2017年ver2.0）
- 近年のサイバーセキュリティ経営を取り巻く情勢の変化等を踏まえ、2022年度中に改訂を実施予定。

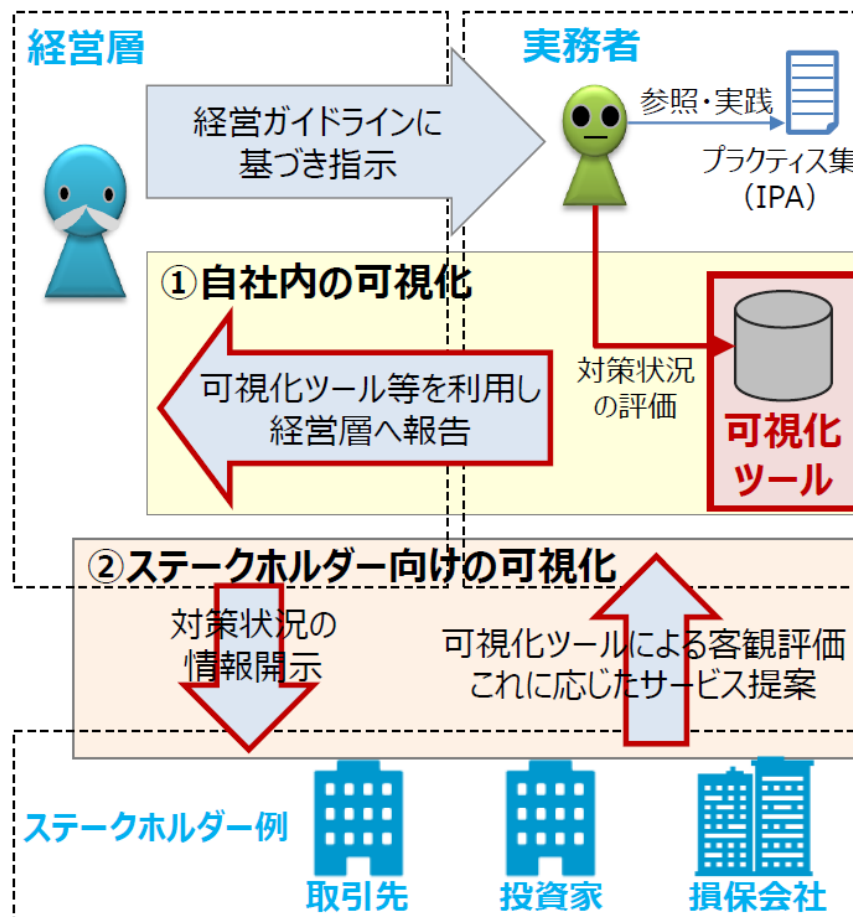
1. 経営者が認識すべき3原則

- (1) 経営者が、リーダーシップを取って対策を進めることが必要
- (2) 自社のみならず、ビジネスパートナーを含めた対策が必要
- (3) 平時及び緊急時のいずれにおいても、関係者との適切なコミュニケーションが必要

2. 経営者がCISO等に指示すべき10の重要事項

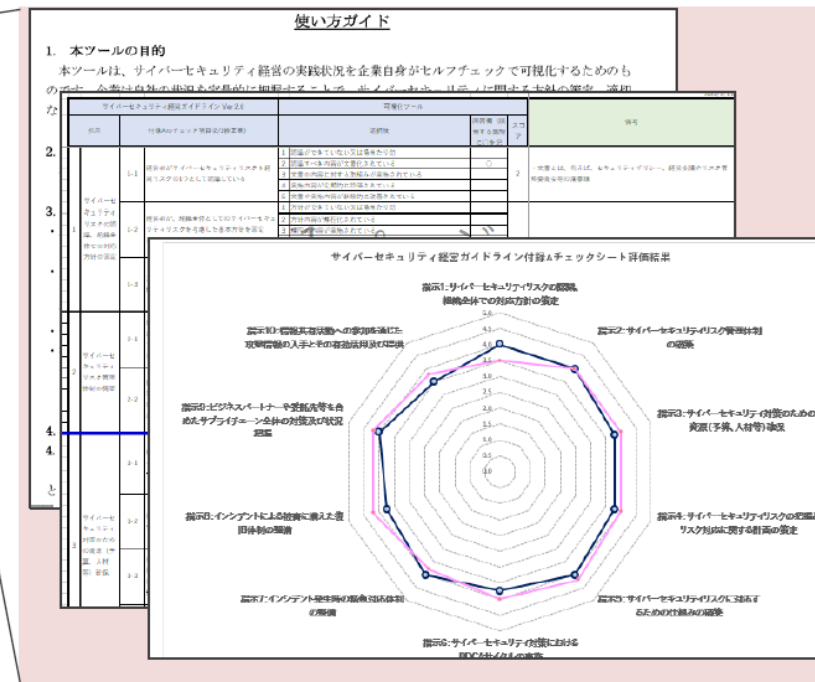
リスク管理体制の構築	指示1	組織全体での対応方針の策定
	指示2	管理体制の構築
	指示3	予算・人材等のリソース確保
リスクの特定と対策の実装	指示4	リスクの把握と対応計画の策定
	指示5	リスクに対応するための仕組みの構築
	指示6	PDCAサイクルの実施
インシデントに備えた体制構築	指示7	緊急対応体制の整備
	指示8	復旧体制の整備
サプライチェーンセキュリティ	指示9	サプライチェーン全体の対策及び状況把握
関係者とのコミュニケーション	指示10	情報共有活動への参加

- 「経営ガイドライン」に基づく指示への対策状況に関し、経営層による自社リスクの可視化や把握、ステークホルダー（取引先、投資家等）とのコミュニケーションに活用できる評価ツール。（2021年8月Web版公開）



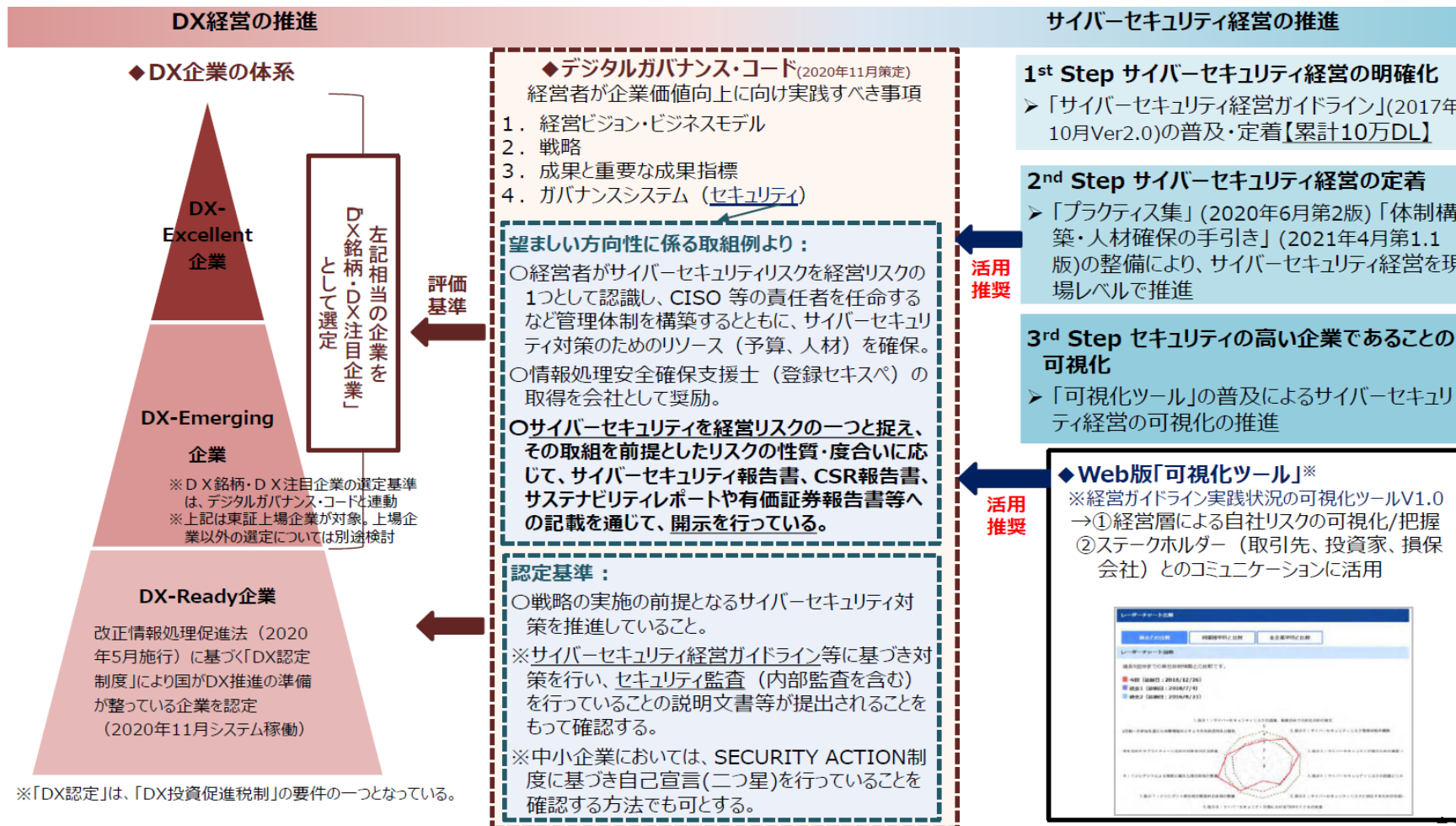
特徴 (Features)

- 39個の質問に回答⇒実践状況をレーダーチャート表示
 - 過去の診断結果とも比較（経年変化）可能※
 - 各業種の平均値とも比較可能※
 - 「サイバーセキュリティ経営ガイドラインVer.2.0実践のためのプラクティス集」の実践事例も表示可能※
- (※β版からの改良点)



<https://www.ipa.go.jp/security/economics/checktool/index.html>

- DXを進める企業におけるステークホルダーとの対話の在り方を示す「デジタルガバナンス・コード」について、「経営者がサイバーセキュリティリスクを経営リスクの1つとして認識」することをはじめ、望ましい方向性に係る取組例等を明記。
- DX投資促進税制の要件の1つとなっている「DX認定制度」の認定基準や、「DX銘柄・DX注目企業」の選定時の評価基準として活用。（インセンティブ）



- 2019年10月にNACD（全米取締役協会）・ISA（米国インターネット・セキュリティ・アライアンス）による「Cyber Risk Oversight Director's Handbook」（米国版ハンドブック）を参考に、すべての取締役役に当てはまる原則を整理。



原則 1	14
取締役は、サイバーセキュリティを、単なるITの問題としてではなく、全社的なリスク管理の問題として理解し、対処する必要がある。	
原則 2	18
取締役は、自社固有の状況と関連付けて、サイバーリスクの法的意味を理解すべきである。	
原則 3	21
取締役会は、サイバーセキュリティに関する十分な専門知識を利用できるようにしておくとともに、取締役会の議題としてサイバーリスク管理を定期的に取り上げ、十分な時間をかけて議論を行うべきである。	
原則 4	26
取締役は、十分な人員と予算を投じて、全社的なサイバーリスク管理の枠組みを確立すべきである。	
原則 5	30
サイバーリスクに関する取締役会における議論の内容として、回避すべきリスク、許容するリスク、保険等によって軽減・移転すべきリスクの特定や、それぞれのリスクへの対処方法に関する具体的計画等を含めるべきである。	

重要インフラ行動計画：取締役等の責任に関する整理

- 重要インフラ事業者に関しては、近日改定予定の「重要インフラのサイバーセキュリティに係る行動計画」において、取締役の責任等に関する整理の記載とともに、「障害対応体制の強化に資する組織統治の在り方について規定化をする」こととした。今後、「安全基準等策定指針」に反映を行い、取組推進を図る。

「重要インフラのサイバーセキュリティに係る行動計画」（抜粋）

IV. 1.1 組織統治の一部としての障害対応体制

（略）重要インフラ事業者等においては、組織の各階層において適切な責任と権限を明確にし、組織一丸となって重要インフラ防護を行う必要があるが、経営層のコミットメントによる組織運営上のリスクのひとつとして、重要インフラ防護の観点を含める必要がある。

内閣官房は、本行動計画において、障害対応体制の強化に資する組織統治の在り方について、安全基準等策定指針において、規定化をする。

重要インフラ事業者等は、本行動計画及び策定された安全基準等策定指針を踏まえ、自組織の障害対応体制の改善に努めるものとする。

(1) 組織統治に必要な観点

組織統治の一部として障害対応体制を強化するためには、「サイバーセキュリティ関係法令Q&AハンドブックVer1.0(令和2年3月2日 内閣官房内閣サイバーセキュリティセンター)」における4つの観点が必要となる。

① 内部統制システムとサイバーセキュリティとの関係

組織におけるサイバーセキュリティに関する体制は、その組織の内部統制システムの一部といえる。経営層の内部統制システム構築義務には、適切なサイバーセキュリティを講じる義務が含まれ得る。

具体的にいかなる体制を構築すべきかは、一義的に定まるものではなく、各組織が営む事業の規模や特性等に応じて、その必要性、効果、実施のためのコスト等様々な事情を勘案の上、各組織において決定されるべきである。また、組織の意思決定機関は、サイバーセキュリティ体制の細目までを決める必要はなく、その基本方針を決定することでもよい。

② サイバーセキュリティと取締役等の責任

組織の意思決定機関が決定したサイバーセキュリティ体制が、当該組織の規模や業務内容に鑑みて適切でなかったため、組織が保有する情報が漏えい、改ざん又は滅失(消失)若しくは毀損(破壊)されたことにより会社に損害が生じた場合、体制の決定に関与した経営層は、組織に対して、任務懈怠(けたい)に基づく損害賠償責任を問われ得る。また、決定されたサイバーセキュリティ体制自体は適切なものであったとしても、その体制が実際には定められたとおりに運用されておらず、経営層(・監査役)がそれを知り、又は注意すれば知ることができたにもかかわらず、長期間放置しているような場合も同様である。

個人情報の漏えい等によって第三者が損害を被ったような場合、経営層・監査役に任務懈怠につき悪意・重過失があるときは、第三者に対しても損害賠償責任を負う。

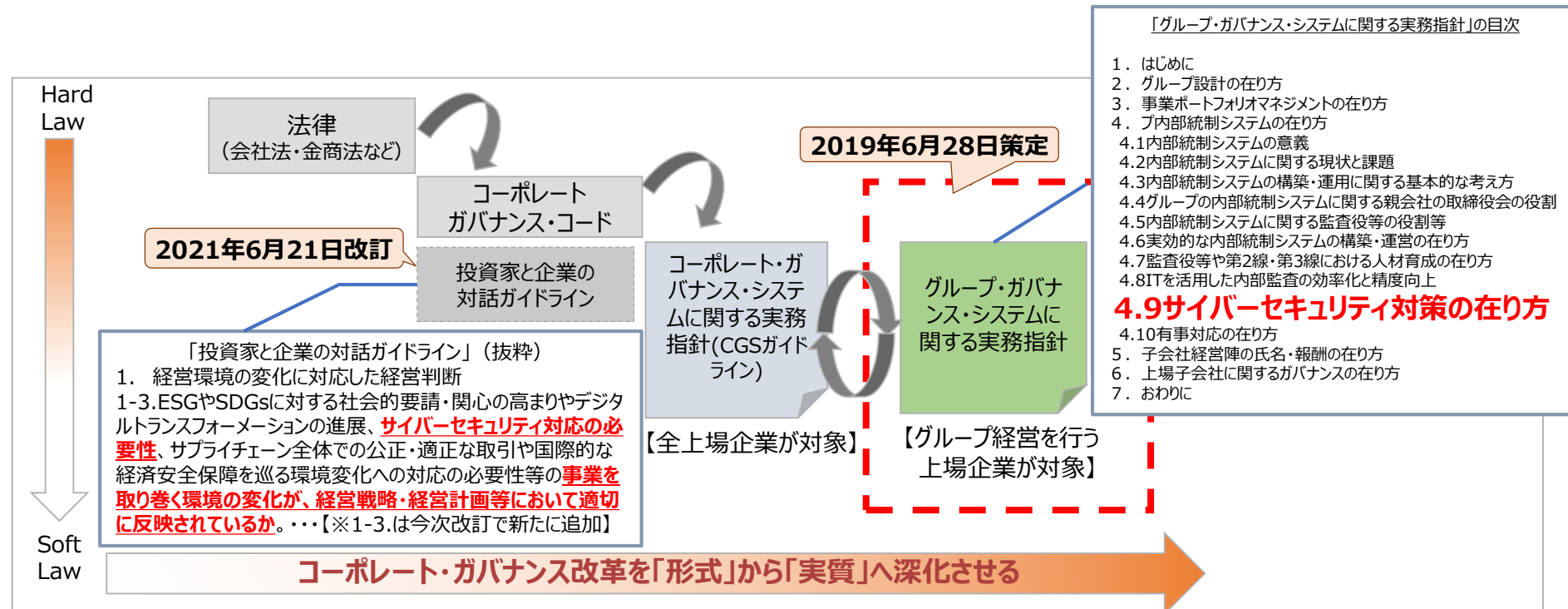
③ サイバーセキュリティ体制の適切性を担保するための監査等（略）

④ サイバーセキュリティと情報開示

サイバーセキュリティに関する組織の情報を開示することは、組織の社会への説明責任を果たすとともに、組織運営上の重要課題としてセキュリティ対策に積極的に取り組んでいるとしてステークホルダーから正当に評価されることが期待できる。また、自組織のサイバーセキュリティ対策の強化もつながることも期待できる。

そこで、組織としては、既存の開示制度を積極的に活用して、サイバーセキュリティに関する取組を開示することが望ましい。

- 2021年6月に改訂された、「スチュワードシップ・コード」及び「コーポレートガバナンス・コード」の附属文書である「投資家と企業の対話ガイドライン」（2021年6月改訂）において、新たに、サイバーセキュリティ対策の必要性等を含む事業環境変化の経営戦略・経営計画等への反映について明記された。



- 日経500社を対象に、総合的に企業のサイバーセキュリティへの取組及び開示姿勢に関する分析を実施。
- また、特に優良であり模範となる企業に星を付与する「格付け」を実施。（2021年度は42社に星を付与）

調査手法

- ・ 調査対象：日経500種平均構成銘柄を構成する500社
- ・ 調査期間：2021年7月～9月上旬
- ・ 総合得点：以下の2項目の合算
- ・ 調査内容：

公開情報

有価証券報告書、コーポレートガバナンス報告書、統合報告書、企業ウェブサイトの記載内容、およびイベント講演、ISMS認証、Pマーク、技術資格取得者数等を調査。



有価証券報告書等

アンケート

公開されていないサイバーセキュリティの取組を確認するため企業へアンケート調査を実施。IPAサイバーセキュリティ可視化ツールを参考に独自の設問を作成。



アンケート調査
(全18問)

- 3/9に米国証券取引委員会 (SEC) が「サイバーセキュリティのリスク管理、戦略、ガバナンス、インシデントの開示に関する規則」の改定を提案。
- 重大なセキュリティインシデント判断後の4営業日以内の情報開示、取締役会メンバーのサイバーセキュリティ専門知識保有状況の開示等を要求する変更が行われている。

改訂事項の一覧

項番	改訂内容
1	登録者が 重大なサイバーセキュリティインシデントを受けたと判断した後、4営業日以内にサイバーセキュリティインシデントに関する情報を開示 するよう要求。
2	以前に開示したサイバーセキュリティインシデントに関する最新情報を提供するよう登録者に要求する。また、これまで未開示だった個別の重要でないサイバーセキュリティインシデントが全体として重要になった場合、経営陣にわかる範囲で、これらのフォームに必要な開示に修正することを提案。
3	以下開示を要求。 ➢ サイバーセキュリティリスクを特定および管理するための登録者のポリシーと手順（ある場合） ➢ サイバーセキュリティリスクに関する取締役会の監督の役割を含む、登録者のサイバーセキュリティガバナンス ➢ サイバーセキュリティ関連のリスクを評価および管理し、関連するポリシー、手順、および戦略を実装する際の管理者の役割と関連する専門知識
4	登録者の 取締役会のメンバーがサイバーセキュリティの専門知識を持っているかどうかについての開示を要求。
5	米国外の企業（「FPI」）にサイバーセキュリティの開示を提供するよう要求。提出する年次報告書は、自国内の開示内容と一致させることを要求。
6	レポートピックとして「サイバーセキュリティインシデント」を追加。
7	開示内容はインラインXBRL形式で提供することを要求。

■ 「サイバーセキュリティ関係法令Q&Aハンドブック」【抜粋】

Q6 サイバーセキュリティと情報開示

(2) 事業報告

会社法第435条第2項に基づき、株式会社は事業報告を作成することが義務付けられている。株式会社は、内部統制システムに関する決定又は決議をしたときは、その決定又は決議の内容の概要及び当該システムの運用状況の概要を事業報告に記載しなければならないところ（会社法施行規則第118条第2号）、サイバーセキュリティに関する事項をこの内部統制システムの一部として開示することが考えられる（サイバーセキュリティと内部統制システムとの関係についてはQ3を参照されたい。）。

(3) 有価証券報告書

金融商品取引法第24条に基づき、有価証券の発行者である会社は、事業年度ごとに、当該会社の商号、当該会社の属する企業集団及び当該会社の経理の状況その他事業の内容に関する重要な事項等について、内閣総理大臣に提出することが義務づけられている。その他事業の内容に関する重要な事項の中には、事業等のリスクが含まれるところ（企業内容等の開示に関する内閣府令第15条第1項第1号に定める第3号様式）、サイバーセキュリティに関するリスクをこの事業等のリスクとして開示することが考えられる。

(4) コーポレート・ガバナンスに関する報告書

証券取引所による開示制度の一環として、コーポレート・ガバナンスに関する報告書が挙げられる。有価証券上場規程（東京証券取引所）第204条第12項第1号等に基づき、新規上場申請者は、コーポレート・ガバナンスに関する基本的な考え方などを記載したコーポレート・ガバナンスに関する報告書を提出することとされている。また、上場後、その内容に変更があった場合は、遅滞なく変更後の報告書を提出することとされている。コーポレート・ガバナンスに関する報告書では、内部統制システムに関する基本的な考え方及びその整備状況を記載することとされているところ（有価証券上場規程施行規則第211条第4項第5号）、サイバーセキュリティに関する事項をこの内部統制システムの一部として開示することが考えられる。

(5) 適時開示

有価証券上場規程第402条等に基づき、上場会社は、剰余金の配当、株式移転、合併の決定を行った場合や災害に起因する損害又は業務遂行の過程で生じた損害が発生した場合等においては、直ちにその内容を開示することとされている。サイバー攻撃に起因して損害が発生する場合には、この災害に起因する損害又は業務遂行の過程で生じた損害として損害・損失の内容や今後の見通しを開示することが考えられる。

サイバーセキュリティ関係法令 Q&A
ハンドブック
Ver1.0

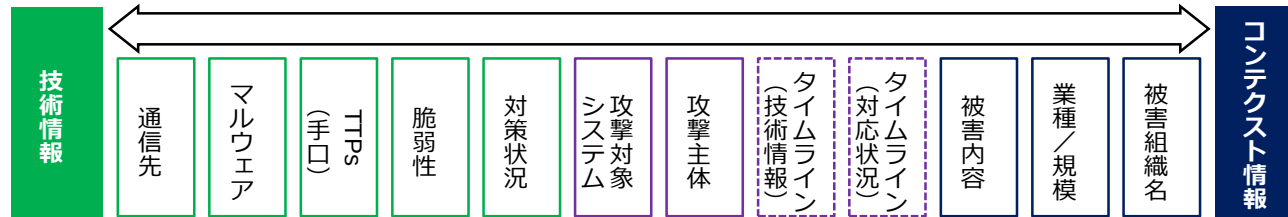
令和2年3月2日
内閣官房内閣サイバーセキュリティセンター（NISC）

〔出典〕NISC「サイバーセキュリティ関係法令Q&A
ハンドブック」（2020年3月）

サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会

- サイバー攻撃被害を受けた組織がサイバーセキュリティ関係組織（例：NISC、警察、所管省庁、JPCERT、ISACなど）と被害に係る情報を共有することは、被害組織自身にとっても社会全体にとっても有益。一方、被害組織においては、どのような情報を、どのタイミングで、どのような主体と共有すべきかについて、必ずしも十分な理解が進んでいない。
 - このため、被害組織の担当部門（例：システム運用部門、法務・リスク管理部門等）を想定読者として、被害組織の立場にも配慮しつつ、サイバー攻撃被害に係る情報を共有する際の実務上の参考となるガイダンス文書を策定し、普及を図ることで、円滑かつ効果的な情報共有を促進していく。
- 検討の場：サイバーセキュリティ協議会^(※)運営委員会下において、サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会を開催し、令和4年中に成案を得る。
※サイバーセキュリティ基本法に基づき、平成31年4月に組織された法定の官民の情報共有体制。関係行政機関で運営委員会を構成。
 - 検討会事務局：警察庁、総務省、経済産業省及びサイバーセキュリティ協議会事務局（NISC及びJPCERT/CC）。

● どのような情報を？（様々な種類・性質の情報が存在）



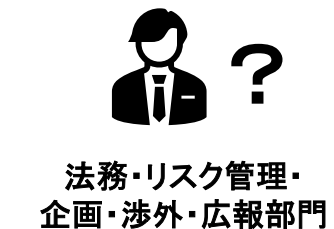
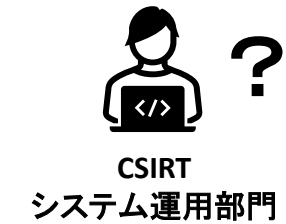
● どのタイミングで？（サイバー攻撃への対処の時系列を意識）



● どのような主体と？（様々なサイバーセキュリティ関係組織が存在）



● 想定読者（被害組織）



- 民間企業のサイバーセキュリティ対策の情報開示の促進のため、民間企業にとって参考となり得る情報開示の事例等をまとめた手引きを策定し、2019年6月に公表。

背景	✓ サイバー攻撃が深刻化する中、民間企業においてサイバーセキュリティ対策は重要な経営課題となっているが、企業としての社会的責任を果たしステークホルダーからの信頼を得るためには、 <u>サイバーセキュリティ対策の実施のみならず、その内容について適切な情報開示が重要。</u>
目的	✓ 民間企業による <u>サイバーセキュリティ対策</u> やその対策の <u>情報開示の重要性</u> の認識を促進。 ✓ 民間企業にとって参考になり得るような <u>既存の情報開示の実例</u> を <u>事例集として</u> 示す。
活用主体	✓ <u>サイバーセキュリティ対策の情報開示</u> に一定の関心のある民間企業の開示の実務担当者等を想定。
対象とする情報開示	✓ <u>開示書類</u> を通じた情報開示を取り扱う。 ✓ 開示書類の読み手は、 <u>投資家、融資元、顧客・契約者・取引先、従業員、競合他社等を含む、社会全体の広範なステークホルダー</u> を想定。
本編 サイバーセキュリティ対策情報開示の手引き	
1. 本手引きの趣旨・目的	【内容】 ✓ サイバーセキュリティリスクの増大と対策の必要性 ✓ サイバーセキュリティ対策の情報開示の意義 ✓ 本手引きの目的、想定参照主体、及び内容・構成等
2. 情報開示の手段	【内容】 ✓ 代表的な開示書類の紹介
3. 企業における情報開示の在り方	【内容】 ✓ 企業において実施されるのが望ましいサイバーセキュリティ対策 ✓ 開示にあたってのポイントと記載例
4. 今後の方向性について	【内容】 ✓ 手引きの改定の在り方等の今後の方向性
参考資料① 関連施策等の紹介	
【内容】	✓ 本手引きに関連した様々な施策やガイドライン等について紹介
参考資料② 開示書類の事例集	
【内容】	✓ サイバーセキュリティ対策の情報開示にかかる実際の開示書類の例について紹介

東京大会に向けたサイバーセキュリティ対策

大会前の対策状況

サイバー攻撃等による影響の未然防止、
軽減に向けた対策等を推進

○リスクアセスメントの取組（事業者等が自主的に実施する取組）

大会に関連する重要サービス事業者等を対象に、リスク評価を実施（2016年から全6回）。

○横断的リスク評価の取組（NISCが評価する取組）

競技会場や特に重要な事業者を対象に、NISCが主体となって検証（2018年から全5回）。

○スポーツ関係団体に対する勉強会

スポーツ関係団体を対象に、サイバーセキュリティに係る勉強会等を開催（2017年から全17回）。

○サイバーインシデント対応演習

現下のサイバーセキュリティ情勢を踏まえたシナリオを用いた演習を実施（2019年から全5回）。

大会開催期間中における 対策の運用等

サイバーセキュリティ対処調整センターを
中心に、インシデント発生時には関係組
織が一丸となって迅速に対処

○情報共有プラットフォームの運用

関係組織間における脅威情報の共有等を迅速・効率的に行うための情報共有プラットフォーム（JISP）を運用。約350の関係組織がJISPを活用。

○サイバーセキュリティ対処調整センターの運用

関係組織からの連絡に即応できるよう24時間態勢（7/9～9/5）で運用。インシデント発生の際には、情報セキュリティ関係機関と協力して、迅速にインシデント対処を支援。

東京大会期間中におけるNISCの活動結果等

対処態勢の概要

- 関係組織との情報共有、相談や報告の受付、インシデント対処等に24時間対応可能な体制を構築・運用
- 個別のインシデント対応を担当するチームを複数構成し、関係組織間でリエゾンの派遣、受け入れを実施

活動結果

大会運営に影響を与えるようなサイバー攻撃は確認されなかった。

大会期間中の主な対応

- インシデント等に対する対処調整
インシデント等を認知した場合、被害組織等との間で、その影響範囲、復旧に向けた対応方針等について情報共有を行い、必要に応じて助言を実施。
インシデント情報等をセキュリティ調整センターとの間で適切に情報共有するとともに、体制参加組織に対してインシデントの発生状況等に関する情報を発信。
- 予防・検知に関する情報の発信・共有
情報セキュリティ関係機関の協力等によって把握した脅威情報について、体制参加組織に注意喚起を実施。
情報セキュリティ関係機関の協力等によって把握した観測情報について、対象組織に個別に連絡し、対処・対策の実施を働きかけ。

大会期間中の主なトピック（大会運営への影響なし）

- ・ サイバー攻撃に関するSNS上の書き込み等
- ・ 米国コンテンツ配信サービス企業における障害
- ・ 不正な動画配信サイト



サイト接続後に案内される不正なアカウント登録画面

東京大会のサイバーセキュリティに関する海外での報道事例について

- 2021年8月17日付の「Security Magazine」にて「The Tokyo Olympics are a cybersecurity success story」と題した記事を掲載（※Security MagazineはBNP Media社が発行）
- 記事は「東京オリンピックはサイバーセキュリティの観点からは本当に成功であり、モデルとして見倣うべきである。」と伝えている。
- 執筆は、Maryville University（米国）のDr. Brian Gant准教授。

記事のポイントは次のとおり。

- ・ 最も良い防御は、良い攻撃である。
(The best defense is a good offense.)
- ・ これまでサイバーセキュリティの分野では、非常に多くの組織が、^(注)攻撃を受けるまで待つという共通の問題があった。
- ・ しかしながら、過去の五輪からの教訓を踏まえ、国際オリンピック委員（IOC）及び東京大会組織委員会（TOC）は同じ過ちを犯さなかった。
- ・ 攻撃者の戦略は絶えず進化しており、我々も過去の栄光に安心することなく、常に緊張感を持ち続けなければならない。
- ・ サイバーセキュリティインシデントが増加する中、東京五輪のような成功例は、明るいニュースとして歓迎すべきであり、消極的な立場に立って過ちを犯しがちな組織にとっては良いモデルになるものである。

The Tokyo Olympics are a cybersecurity success story



ISMAP制度と現在の取組（ISMAP-LIU）

政府情報システムのためのセキュリティ評価制度（以下「ISMAP」という。）は、政府機関等がクラウドサービスを調達する際、ISMAPクラウドサービスリストに登録されたサービスから調達することを原則とする制度として令和2年6月より開始。現在※25社34サービスが登録中

※令和4年6月1日時点

- ISMAPの対象となっている機密性2情報を扱う情報システムは IaaS、PaaS、SaaSと多岐にわたる。
- 中でもSaaSはサービスの幅が広く、用途や機能が極めて限定的なサービスや、機密性2情報の中でも比較的重要度が低い情報のみを取り扱うサービス等リスクが低いサービスもあり、それらのサービスについて現行のISMAPと一律の取扱いとした場合、過剰なセキュリティ要求となり、それにより当該サービスの活用が進まない場合も考えられる。
- このため、機密性2情報を扱うSaaSのうち、セキュリティ上のリスクの小さな業務・情報の処理に用いるものに対する仕組みを創設することとし、現行ISMAPの枠組みをベースとして、外部監査対象範囲の縮小を含め、想定される各論点について検討を行ったもの。
- あわせて、ISMAP-LIU（注）の検討結果を踏まえ、新規の暫定措置期間のうち類型②について、クラウドサービスの登録申請の状況や各政府機関等におけるニーズを踏まえつつ、制度の利用推進の観点からの見直し要否の検討を行った。

ISMAP-LIUの基本構成

- ISMAP-LIUの対象は、SaaSの中でもセキュリティ上のリスクの小さな業務・情報の処理に用いるもの。
- ISMAP-LIU該当性の判断に当たっては、**利用する各省庁における業務・情報の影響度※評価の提出を必須とし、実ケースとして影響度の低い業務に用いられるSaaSであることを確認。**
※業務・情報の影響度は、クラウドサービスで取り扱われ処理される各種情報において、機密性・完全性・可用性が損なわれた場合の影響度を示す。
- その際、CSP、各省庁による効率的な申請・業務・情報の影響度評価を促すため、**ISMAP-LIUにおける業務・情報の影響度が低位である蓋然性が高い業務（対象業務一覧）を提示**することを想定。

「対象業務一覧」の考え方

- － 「対象業務一覧」に該当する業務の場合：
CSPや利用省庁等が申請、業務・情報の影響度評価を行う際の参考として、ISMAP-LIUにおける業務・情報の影響度が低位である蓋然性が高い業務を例示したものであり、対象業務一覧に該当する業務に用いるSaaSに係る事前申請はLIU対象として扱う。
- － 「対象業務一覧」に該当しない業務の扱い：
対象業務一覧に該当しない業務（要検討業務）に用いるSaaSについては、CSPからの事前申請を受け付けた上で当該業務に係わる業務・情報の影響度評価の結果が低位であることの妥当性を、複数の省庁(2省庁を想定)の結果から判断する。低位である妥当性が確認された業務については、順次、対象業務一覧に追加する。
要検討業務の判断については、一定の処理期間を設ける。

